SHORT PROJECT

Comprehensive Security Assessment and Hardening Report for Small Business Network

HAFIZ NAVEED UDDIN

SUMMERY

CYBER SECURITY INTERN

Comprehensive Security Assessment and Hardening Report for Small Business Network

This project is designed for a comprehensive security assessment and hardening of a small business network. The objective of the assessment is to map the network topology, identify connected devices, detect vulnerabilities, and implement security measures to mitigate risks.

Case

1. **Introduction** Project Overview This project is designed for a comprehensive security assessment and hardening of a small business network. The objective of the assessment is to map the network topology, identify connected devices, detect vulnerabilities, and implement security measures to mitigate risks.

   Objectives

   - Understand the network topology.
   - Identify all connected devices and document their details.
   - Perform a vulnerability scan on the network and document the findings.
   - Summarize the current state of network security.
   - Provide recommendations for security improvements.
2. **Network Topology** Network Diagram (Include network diagram here)

   Connected Devices List

IP Address	MAC Address	Device Role	Operating System	Installed Software	Firmware Version	Service Packs
192.168.0.2	00:1A:2B:3C:4D:5E	Workstation	Windows 11	Microsoft Office, Adobe Reader	1.0	SP1
192.168.0.3	00:1A:2B:3C:4D:5F	Router	Firmware v2.1	N/A	2.1	N/A
192.168.0.4	00:1A:2B:3C:4D:5G	Server	Ubuntu Server 20.04	Apache, MySQL	N/A	N/A
192.168.0.5	00:1A:2B:3C:4D:5H	IoT Device	Custom Firmware	N/A	1.0	N/A

3. **Inventory of Assets Hardware Inventory**

Device Name	Type	Model	Serial Number	Location
Workstation1	Workstation	Dell OptiPlex 7010	SN123456	Office 1
Router1	Router	Cisco RV340	SN789012	Server Room
Server1	Server	HP ProLiant DL360	SN345678	Server Room

Device Name	Type	Model	Serial Number	Location
IoTDevice1	IoT Device	Raspberry Pi 4	SN901234	Office 2

4. **Software Inventory**

Device Name	Software	Version	License Status
Workstation1	Microsoft Office	2019	Licensed
Workstation1	Adobe Reader	2020	Licensed
Server1	Apache	2.4.41	Open Source
Server1	MySQL	8.0.21	Open Source

5. **Vulnerability Scan Results Identified Vulnerabilities**

Device Name	Vulnerability	Risk Level	Description	Recommendation
Workstation1	CVE-2021-34527	High	Print Spooler Remote Code Execution Vulnerability	Apply latest security patches
Router1	Default Password	Medium	Router using default admin password	Change the default password
Server1	Open Ports	Medium	Multiple unnecessary open ports	Close unnecessary ports
IoTDevice1	Outdated Firmware	High	IoT device firmware is outdated	Update to latest firmware

6. **Summary of Findings Current Security State** The overall security state of the network is moderate, but there are some critical vulnerabilities that need immediate attention. The network topology is clear, and devices have been correctly identified. The asset inventory is complete, and the vulnerability scan results have highlighted some significant issues.

Major Issues

- Print Spooler Remote Code Execution Vulnerability on Workstation1
- Default admin password on Router1
- Multiple unnecessary open ports on Server1
- Outdated firmware on IoTDevice1

7. **Recommendations Immediate Actions**
   - Workstation1: Apply the latest security patches to fix the Print Spooler vulnerability.
   - Router1: Change the default admin password to a strong, unique password.
   - Server1: Close all unnecessary open ports.
   - IoTDevice1: Update the firmware to the latest version.

Long-term Strategies

- Regular Updates: Ensure all systems are regularly updated with the latest security patches.
- Periodic Assessments: Conduct regular security assessments to identify new vulnerabilities.
- User Training: Conduct security awareness training for all employees to prevent social engineering attacks.
- Network Monitoring: Implement continuous network monitoring to detect suspicious activities promptly.

Conclusion Completion of Phase 1 has enhanced the network's security posture and addressed vulnerabilities. Await comprehensive report for further details on experiences and results from Phase 2, Phase 3, and Phase 4.